AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Property located at 703 107th Pl. SW, Everett, Washington 98204, more fully described in Attachment A	)	Case No. MJ20-292

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Property located at 703 107th Pl. SW, Everett, Washington 98204, more fully described in Attachment A

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C §§ 841(a)(1); 846; 843(b); 18 U.S.C. § 1956	Distribution of Controlled Substances; Conspiracy to Distribute Controlled Substances; Use of a Communications Facility in Furtherance of a Felony Drug Offense; Conspiracy to Launder Monetary Instruments.

The application is based on these facts:

✓ See Affidavit of Special Agent Joshua W. Kent, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days: _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Joshua W. Kent, DEA Special Agent

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

⊙ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: May 28, 2020

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

USAO# 2020R00511

AFFIDAVIT OF JOSHUA W. KENT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Joshua W. Kent, a Special Agent with the Drug Enforcement Administration, Honolulu, Hawaii, having been duly sworn, state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am employed as a Special Agent (SA) with the United States Drug Enforcement Administration (DEA), and have been so employed since June 2019. I am currently assigned to the Honolulu District Office and, specifically, the Honolulu High Intensity Drug Trafficking Area (HIDTA) Task Force. In this capacity, I investigate violations of the Controlled Substance Act, Title 21, United States Code, Section 801 et seq., and related offenses. I have received specialized training in the enforcement and investigation of the Controlled Substance Act. Prior to entering the DEA, I was a Child Protective Investigator for the Hillsborough County Sheriff's Office.

2. I have become knowledgeable with the enforcement of federal laws pertaining to narcotics and dangerous drugs. I attended and successfully completed the Basic Agent training program necessary to become a certified Special Agent at the DEA Academy in Quantico, Virginia. I have been involved in numerous drug related arrests and surveillances operations. I have participated in drug trafficking investigations in which court-authorized wire interception was utilized.

3. In my role as a Special Agent for the Drug Enforcement Administration, I have conducted and/or participated in investigations that resulted in the seizure of various quantities of methamphetamine, heroin, lysergic acid diethylamide ("LSD"), marijuana, other controlled substances, and of narcotic proceeds. Based on my training and experience, I have become well versed in the methodology utilized in narcotics trafficking operations, the specific types of language used by narcotic traffickers, the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

unique trafficking patterns employed by narcotics organizations and their patterns of drug abuse.

II. PURPOSE OF AFFIDAVIT

4. This application seeks permission to search the following location, which is more particularly described in Attachment A, attached hereto and incorporated by this reference as if set forth fully herein. As summarized herein, the location is believed to be utilized by one or more participants in the crimes described herein, and there is probable cause to believe evidence of those crimes will be found at the following location:

a. **703 107th Pl. SW, Everett, Washington 98204:** Hereinafter referred to as the "**target location**," as well as any digital devices or other electronic storage media located therein. Investigators believe the **target location** is utilized by Devin Vassallo.

5. I believe the **target location** is presently being used in the Western District of Washington in furtherance of the following federal criminal offenses: 21 U.S.C. § 841(a)(1), Distribution of Controlled Substances, 21 U.S.C. § 846, Conspiracy to Distribute Controlled Substances, 21 U.S.C. § 843(b), Use of a Communications Facility in Furtherance of a Felony Drug Offense, and 18 U.S.C. § 1956(h), Conspiracy to Launder Monetary Instruments.

6. I have obtained the facts set forth in this affidavit through my personal participation in the investigation described below; from oral and written reports of other law enforcement officers; and from records, documents and other evidence obtained during this investigation. I have obtained and read official reports prepared by law enforcement officers participating in this investigation and in other investigations by the DEA. Insofar as I have included event times in this affidavit, those event times are approximate.

7. Since this affidavit is being submitted for the limited purpose of obtaining authority to search the **target location**, I have not included every fact known concerning this investigation. I have set forth only the facts that I believe are essential for a fair

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

determination of probable cause that the target subject is involved in drug trafficking, and the **target location** is being used to facilitate that drug trafficking.

III. SUMMARY OF INVESTIGATION

8. The DEA is investigating Devin Vassallo, a 24-year-old resident of Everett, Washington, who distributes narcotics, including LSD, 3,4-Methylenedioxymethamphetamine (more commonly known as MDMA), and marijuana, in the Western District of Washington. Through the use of a cooperating defendant ("the CD"), investigators have obtained evidence that Vassallo distributes LSD and other controlled substances from the Western District of Washington to the island of Oahu in the District of Hawaii.

IV. PROBABLE CAUSE FOR SEARCHING THE TARGET LOCATION

9. On May 19, 2020, the CD, who had been arrested for distributing LSD in Hawaii, provided information on an individual known to the CD as Devin Vassallo. The CD advised that s/he knew Vassallo from when the CD previously lived in Washington and has met Vassallo multiple times at the **target location**, which the CD understands to be Vassallo's residence.

The CD told investigators that since 2017, Vassallo has been his/her source of supply for LSD, marijuana, and MDMA. Vassallo supplies the CD with narcotics via shipments through the United States Postal Service from Washington to Hawaii. According to the CD, Vassallo sent her/him parcels containing controlled substances on a weekly to biweekly basis. The CD advised Vassallo was sending multi-pound quantities of marijuana, multiple vials of LSD liquid, ounce quantities of MDMA, and multi-ounce to pound quantities of mushrooms. The CD advised that s/he paid for these controlled substances primarily by sending cash through USPS to Vassallo. The CD also advised he/she has sent money through Venmo and MoneyGram Walmart to pay for these controlled substances.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. The CD showed investigators a "Signal" conversation between the CD and Vassallo. Signal is an end-to-end encrypted communications platform, which is known to commonly be used by drug traffickers to avoid detection by law enforcement. Signal can be used through either a phone-based application or a desktop-based application. The Signal conversation between the CD and Vassallo was comprised of several months of communications discussing drug transactions, to include a specific parcel being seized by USPS in late March, 2020. In this instance, Vassallo and the CD refer to the seized parcel by the fake name on its label. The conversation also includes screenshots of the notice of seizure from the postal service. In the conversation, Vassallo said that this specific parcel contained marijuana and mushrooms.

11. The most recent "Signal" conversation between the CD and Vassallo discussed a package sent to the CD's post office box.

12. The CD also provided that on May 4, 2020, the CD ordered LSD from Vassallo to be sent via USPS to the CD's UPS post office box in Hawaii. With investigators present, the CD contacted Vassallo through a Snapchat account named "dabbindevin." The CD confirmed that this Snapchat account belonged to Vassallo. Vassallo responded and told the CD that the LSD ordered on May 4, 2020 was sent to the UPS post office box.

13. Later on May 19, 2020, investigators searched the CD's post office box and seized a parcel containing suspected LSD on water color paper that originated from a post office in Everett, Washington. This suspected LSD paper matched details of the content of the Signal conversation between the CD and Vassallo and seen by investigators.

14. The CD indicated that s/he sent money via USPS to a post office box in Washington registered to a "Stefan D'Alesandro." This information was corroborated through the "Signal" messages between the CD and Vassallo. The CD advised that D'Alessandro is a roommate of Vassallo.

15. The CD positively identified Vassallo from a Snapchat video and from Vassallo's Washington driver license photograph. The CD advised that the Snapchat

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

video, which is approximately two seconds long, was taken a few years ago by the CD personally. The CD identified Vassallo's residence as the **target location** from Google Maps images. The CD further confirmed the address from the CD's Amazon transaction history, in which the CD has sent drug paraphernalia in packages to Vassallo at the **target location**. The most recent of these shipments was on May 4, 2020.

16. The CD said Vassallo lives at the **target location** with Vassallo's father. Snohomish County property records show that the **target location** is owned by Mark Vassallo, Devin Vassallo's father. The CD told investigators that s/he knows Vassallo stores narcotics at the **target location**.

V. KNOWLEDGE BASED ON TRAINING AND EXPERIENCE

17. Based on my training and experience, and my discussions with other experienced officers and agents involved in drug investigations, I know the following:

a. During the execution of search warrants, it is common to find papers, letters, billings, documents, and other writings that show ownership, dominion, and control of vehicles, residences, and/or storage units.

b. It is common for drug dealers to secrete contraband, proceeds of drug sales, and records of drug transactions in secure locations within their vehicles, residences, and/or storage units for their ready access and to conceal them from law enforcement.

c. Narcotics traffickers maintain books, records, receipts, notes, ledgers, airline tickets, money orders, and other papers relating to the transportation, ordering, sale, and distribution of controlled substances. Narcotics traffickers commonly "front," that is, provide on consignment, controlled substances to their clients. These books, records, receipts, notes, and ledgers, commonly known as "pay and owe sheets," are maintained where traffickers have ready access to them.

d. Traffickers of controlled substances, and those who assist them, maintain and tend to retain accounts or records of their drug trafficking activities, including lists of drug quantities and money owed, telephone records including contact names and numbers, photographs, and similar records of evidentiary value. These items are generally kept in locations where drug traffickers believe their property is secure and will remain undetected from law enforcement, such as inside their homes and vehicles.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Sometimes, these locations are not their primary residence, but instead used for the purposes of storing and distributing drugs.

e. Traffickers of controlled substances commonly maintain records reflecting names or nicknames, addresses, vehicles, and/or telephone numbers of their suppliers, customers and associates in the trafficking organization. Traffickers commonly maintain this information in books or papers as well as in cellular telephones and other electronic devices. Traffickers often maintain cellular telephones for ready access to their clientele and to maintain their ongoing narcotics business. Traffickers frequently change their cellular telephone numbers to avoid detection by law enforcement, and it is common for traffickers to use more than one cellular telephone at any one time.

f. Traffickers maintain evidence of their criminal activity at locations that are convenient to them, including their residences and vehicles. This evidence often includes more than contraband and paraphernalia and includes financial records, records of property and vehicle ownership, records of property rented, records of storage facilities used to hide drugs or currency, and other documentary evidence relating to commission of, and proceeds from, their crimes. Narcotics traffickers sometimes take or cause to be taken photographs and/or video recordings of themselves, their associates, their property, and their illegal product, or have photo or video security systems that record images from their homes or property. These individuals usually maintain these photographs and recordings in their possession or at their premises, in a safe place. Such evidence may be kept at a safe location for a long time after the drug deal(s) to which they pertain are completed, if the location remains under the control of the trafficker.

g. Traffickers frequently maintain items necessary for weighing, packaging and cutting drugs for distribution. This paraphernalia often includes, but is not limited to, scales, plastic bags and other packaging materials, sifters, containers, and cutting/diluting agents and items to mask the odor of narcotics. Persons trafficking and using controlled substances frequently sell more than one type of controlled substance at any one time.

h. It is common for drug dealers to also be users of their product, and it is common for drug users to maintain paraphernalia associated with the use of controlled substances, such as syringes, pipes, spoons, containers, straws, and razor blades.

i. Traffickers frequently maintain records, books, notes, ledgers, travel documents, and other papers relating to the transportation and distribution of controlled substances in locations convenient to them, such as their residences and vehicles.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

j. Traffickers often maintain weapons, including firearms and ammunition, in secure locations such as their residences and vehicles, in order to protect their drugs and drug proceeds.

k. Traffickers often have false identification documents and identification documents in the names of others. Traffickers very often place assets in names other than their own, or use fictitious names and identification, to avoid detection of these assets by government agencies, while continuing to use these assets and exercise dominion and control over them.

l. Drug trafficking is a cash business, often involving large amounts of cash at any one time, so drug traffickers often have money counters.

m. Persons involved in drug trafficking conceal in their residences caches of drugs, large amounts of currency, financial instructions, precious metals, jewelry, and other items of value and/or proceeds of drug transactions as well as evidence of financial transactions relating to obtaining, transferring, secreting, or the spending of large sums of money made from engaging in narcotics trafficking activities.

o. Unexplained wealth is probative evidence of crimes motivated by greed, in particular, trafficking in controlled substances.

q. Illegal drug trafficking is a continuing activity over months and even years. Illegal drug traffickers will repeatedly obtain and distribute controlled substances on a somewhat regular basis, much as any distributor of a legitimate commodity would purchase stock for sale, and, similarly, drug traffickers will have an "inventory," which fluctuates in size depending upon various factors, including the demand and supply for the product. I would expect the trafficker to keep records of his illegal activities for a period of time extending beyond the time during which he actually possesses illegal controlled substances, in order that he can maintain contact with his criminal associates for future drug transactions, and so that he can have records of prior transactions for which, for example, he might still be owed money, or might owe someone else money. These records are often created in code.

r. Drug trafficking is a cash business, and in order to escape notice from authorities for using unexplained income, or hide excessive cash from illegal activities, traffickers either keep large quantities of cash at home or other secure locations, such as safe deposit boxes, or convert the cash into other valuable assets, such as jewelry, precious metals, monetary instruments, or other negotiable forms of wealth. Records of such conversions are often stored where a trafficker lives or in other secure locations such as safe deposit boxes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

s. Money launderers often have banking records to include but not limited to, deposit or withdrawal slips, bank statements, checks, or money orders. Some of these banking records may not be in their own name. Money launderers often have several accounts documented in some form, or instructions detailing how to handle each respective account. For example, they may have a list of accounts belonging to several different people with instructions for how much to deposit or withdraw from each and often maintain this information for long periods of time in their residences or safe deposit boxes.

t. Money launderers often have records or evidence related to how the proceeds were spent or concealed and often maintain this information for long periods of time in their residences or safe deposit boxes. Evidence may include jewelry and/or vehicles, as well as the contents of storage lockers, safe deposit boxes or bank accounts. The use of bank accounts is a common money movement technique used by drug traffickers to receive payment for narcotics from customers outside of their geographic region. It is common for a trafficker to use several bank accounts for this purpose simultaneously in an attempt to avoid detection by the financial institutions and/or law enforcement. The use of multiple accounts, and the commingling of illicit funds with legitimate funds in particular, is often part of the plan to conceal the illegal activity or may be part of the overall integration mechanism by which the illicit funds are made to appear as part of the legitimate income so that only a small portion of or even none of the funds from an account are seized.

18. Based on my training and experience, and that of those around me, I also know that drug dealers use cellular telephones as a tool or instrumentality in committing their criminal activity, to include laundering their proceeds. They use them to maintain contact with their suppliers, distributors, and customers. They prefer cellular telephones because, first, they can be purchased without the location and personal information that land lines require. Second, they can be easily carried to permit the user maximum flexibility in meeting associates, avoiding police surveillance, and traveling to obtain or distribute drugs. Third, they can be passed between members of a drug conspiracy to allow substitution when one member leaves the area temporarily. Since cellular phone use became widespread, every drug dealer I have contacted has used one or more cellular telephones for his or her drug business. I also know that it is common for drug traffickers to retain in their possession phones that they previously used, but have discontinued actively using, for their drug trafficking business. These items may be kept for months

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and months in a safe place controlled by the drug trafficker. Based on my training and experience, the data maintained in a cellular telephone used by a drug dealer is evidence of a crime or crimes. This includes the following:

a. The assigned number to the cellular telephone (known as the mobile directory number or MDN), and the identifying telephone serial number (Electronic Serial Number, or ESN), (Mobile Identification Number, or MIN), (International Mobile Subscriber Identity, or IMSI), or (International Mobile Equipment Identity, or IMEI) are important evidence because they reveal the service provider, allow us to obtain subscriber information, and uniquely identify the telephone. This information can be used to obtain toll records, to identify contacts by this telephone with other cellular telephones used by co-conspirators, to identify other telephones used by the same subscriber or purchased as part of a package, and to confirm if the telephone was contacted by a cooperating source.

b. The stored list of recent received, missed, and sent calls is important evidence. It identifies telephones recently in contact with the telephone user. This is valuable information in a drug investigation because it will identify telephones used by other members of the organization, such as suppliers, distributors and customers, and it confirms the date and time of contacts. If the user is under surveillance, it identifies what number he called during or around the time of a drug transaction or surveilled meeting. Even if a contact involves a telephone user not part of the conspiracy, the information is helpful (and thus is evidence) because it leads to friends and associates of the user who can identify the user, help locate the user, and provide information about the user. Identifying a defendant's law-abiding friends is often just as useful as identifying his drug-trafficking associates.

c. Stored text messages are important evidence, similar to stored numbers. Agents can identify both drug associates, and friends of the user who likely have helpful information about the user, his location, and his activities.

d. Drug traffickers increasingly use applications on smart phones that encrypt communications, such as Signal, or applications that automatically delete messages, such as Snapchat, in order to avoid law enforcement monitoring or recording of communications regarding drug trafficking and/or money laundering. Evidence of the use of such applications can be obtained from smart phones, and is evidence of a smart phone user's efforts to avoid law enforcement detection.

e. Photographs on a cellular telephone are evidence because they help identify the user, either through his or her own picture, or through pictures of friends, family, and associates that can identify the user. Pictures also identify associates likely to be members of the drug trafficking organization. Some drug dealers photograph groups

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of associates, sometimes posing with weapons and showing identifiable gang signs. Also, digital photos often have embedded "geocode" or GPS information embedded in them. Geocode information is typically the longitude and latitude where the photo was taken. Showing where the photo was taken can have evidentiary value. This location information is helpful because, for example, it can show where coconspirators meet, where they travel, and where assets might be located.

f. Stored address records are important evidence because they show the user's close associates and family members, and they contain names and nicknames connected to phone numbers that can be used to identify suspects.

VI. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the **target location**, in whatever form they are found. One form in which the evidence and/or instrumentalities might be found is data stored on digital devices[1] such as computer hard drives or other electronic storage media.[2] Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

20. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the **target location**, there is probable

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cause to believe that evidence and/or instrumentalities of the crimes of 21 U.S.C. § 841(a)(1), Distribution of Controlled Substances, 21 U.S.C. § 846, Conspiracy to Distribute Controlled Substances, 21 U.S.C. § 843(b), Use of a Communications Facility in Furtherance of a Felony Drug Offense, and 18 U.S.C. § 1956(h), Conspiracy to Launder Monetary Instruments, will be stored on those digital devices or other electronic storage media. I believe digital devices or other electronic storage media are being used to facilitate communications between Vassallo and the CD over Signal for the purpose of shipping drugs from Washington to Hawaii and to coordinate the deliveries and payments supporting said drug trafficking. There is, therefore, probable cause to believe that evidence and/or instrumentalities of the crimes of 21 U.S.C. § 841(a)(1), Distribution of Controlled Substances, 21 U.S.C. § 846, Conspiracy to Distribute Controlled Substances, 21 U.S.C. § 843(b), Use of a Communications Facility in Furtherance of a Felony Drug Offense, and 18 U.S.C. § 1956, Conspiracy to Launder Monetary Instruments, exists and will be found on digital device or other electronic storage media at the **target location**, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the **target location** because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[3] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is

---

[3] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

VII. DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

22. The investigation indicates that Vassallo uses digital devices as an instrumentality of his drug trafficking activity. The CD showed investigators a Signal conversation between the CD and Vassallo discussing a drug shipment sent to the CD's post office box.

VIII. PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION

23. Because of the nature of the evidence that I am attempting to obtain and the nature of the investigation, I have not made any prior efforts to obtain the evidence based on the consent of any party who may have authority to consent. I believe, based upon the nature of the investigation and the information I have received, that if Vassallo becomes aware of the investigation in advance of the execution of a search warrant, he may attempt to destroy any potential evidence, whether digital or non-digital, thereby hindering law enforcement agents from the furtherance of the criminal investigation. In addition, because Vassallo uses encrypted forms of communication, such as Signal, the only practical way to obtain a comprehensive set of Vassallo's communications regarding his drug trafficking and money laundering is to search his cell phone.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

IX. RISK OF DESTRUCTION OF EVIDENCE

24. I know based on my training and experience that digital information can be very fragile and easily destroyed. Digital information can also be easily encrypted or obfuscated such that review of the evidence would be extremely difficult, and in some cases impossible. In the instant case, I know based on communications provided by the CD, that Vassallo uses encrypted communications to engage in his crimes. Accordingly, he may use encryption on the computer systems he utilizes to engage in his crimes. If an encrypted computer is either powered off or if the user has not entered the encryption password and logged onto the computer, it is likely that any information contained on the computer will be impossible to decipher. If the computer is powered on, however, and the user is already logged onto the computer, there is a much greater chance that the digital information can be extracted from the computer. This is because when the computer is on and in use, the password has already been entered and the data on the computer is accessible. However, giving the owner of the computer time to activate a digital security measure, pull the power cord from the computer, or even log off of the computer could result in a loss of digital information that could otherwise have been extracted from the computer.

X. REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

25. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

XI. SEARCH TECHNIQUES

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. Because multiple people share the **target location** as a residence, it is possible that the **target location** will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

28. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

A. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.[4]

[4] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

B. Searching the Forensic Images.

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those

---

generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

XII. REQUEST FOR SEALING

29. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, affidavit and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation and disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Disclosure of these materials would give the target of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

XIII. CONCLUSION

30. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of the crimes of 21 U.S.C. § 841(a)(1), Distribution of Controlled Substances, 21 U.S.C. § 846, Conspiracy to Distribute Controlled Substances, 21 U.S.C. § 843(b), Use of a Communications Facility in Furtherance of a Felony Drug Offense, and 18 U.S.C. § 1956(h), Conspiracy to Launder Monetary Instruments, are located at the **target location**, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found at the **target location**. I therefore request that the court issue a warrant authorizing a search of the **target location**, as well as any digital devices and electronic storage media located therein, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

JOSHUA W. KENT
Special Agent, DEA

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 28th day of May, 2020.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A
PROPERTY TO BE SERACHED

703 107th Pl. SW, Everett, Washington 98204 – Referred to herein as the "**target location**." The location is a one story, single-family residence that is brown in color with a concrete slab driveway leading to a garage that fronts the house. The numbers "703" are affixed to the wall beside the front door.

And any digital device/s or other electronic storage media found therein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This warrant authorizes the government to search for the following items:

Evidence and/or fruits of the commission of the following crimes: Distribution and Possession with Intent to Distribute Controlled Substances, to wit, LSD, MDMA, and marijuana in violation of 21 U.S.C. § 841(a)(1); Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances, in violation of 21 U.S.C. § 846; Use of a Communications Facility in Furtherance of a Felony Drug Offense in violation of 21 U.S.C. § 843(b); and Conspiracy to Launder Monetary Instruments in violation of 18 U.S.C. § 1956, including but not limited to the following:

1. Controlled Substances: Including but not limited to LSD, MDMA, and marijuana.

2. Drug Paraphernalia: Items used, or to be used, to store, process, package, use, and/or distribute controlled substances, such as plastic bags, cutting agents, scales, measuring equipment, tape, hockey or duffel bags, chemicals or items used to test the purity and/or quality of controlled substances, and similar items.

3. Drug Transaction Records: Documents such as ledgers, receipts, notes, and similar items relating to the acquisition, transportation, and distribution of controlled substances.

4. Customer and Supplier Information: Items identifying drug customers and drug suppliers, such as telephone records, personal address books, correspondence, diaries, calendars, notes with phone numbers and names, "pay/owe sheets" with drug amounts and prices, maps or directions, and similar items.

5. Cash and Financial Records: Currency and financial records, including bank records, safe deposit box records and keys, credit card records, bills, receipts, tax returns, vehicle documents, and similar items; and other records that show income and expenditures, net worth, money transfers, wire transmittals, negotiable instruments, bank drafts, cashiers checks, and similar items, and money counters.

6. Photographs/Surveillance: Photographs, video tapes, digital cameras, surveillance cameras and associated hardware/storage devices, and similar items, depicting property occupants, friends and relatives of the property occupants, or

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

suspected buyers or sellers of controlled substances, controlled substances or other contraband, weapons, and assets derived from the distribution of controlled substances.

7. Weapons: Including but not limited to firearms, magazines, ammunition, and body armor.

8. Codes: Evidence of codes used in the distribution of controlled substances, including but not limited to passwords, code books, cypher or decryption keys, and similar information.

9. Property Records: Deeds, contracts, escrow documents, mortgage documents, rental documents, and other evidence relating to the purchase, ownership, rental, income, expenses, or control of the premises, and similar records of other property owned or rented.

10. Indicia of occupancy, residency, and/or ownership of assets including, but not limited to, utility and telephone bills, canceled envelopes, rental records or payment receipts, leases, mortgage statements, and other documents.

11. Evidence of Storage Unit Rental or Access: rental and payment records, keys and codes, pamphlets, contracts, contact information, directions, passwords or other documents relating to storage units.

12. Evidence of Personal Property Ownership: Registration information, ownership documents, or other evidence of ownership of property including, but not limited to vehicles, vessels, boats, airplanes, jet skis, all terrain vehicles, RVs, and personal property; evidence of international or domestic travel, hotel/motel stays, and any other evidence of unexplained wealth,

13. All bearer bonds, letters of credit, money drafts, money orders, cashier's checks, travelers checks, Treasury checks, bank checks, passbooks, bank drafts, money wrappers, stored value cards, and other forms of financial remuneration evidencing the obtaining, secreting, transfer, and/or concealment of assets and/or expenditures of money.

14. All Western Union and/or Money Gram documents and other documents evidencing domestic or international wire transfers, money orders, official checks, cashier’s checks, or other negotiable interests that can be purchased with cash, These

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

documents are to include applications, payment records, money orders, frequent customer cards, etc.

15. Negotiable instruments, jewelry, precious metals, financial instruments, and other negotiable instruments.

16. Documents reflecting the source, receipt, transfer, control, ownership, and disposition of United States and/or foreign currency.

17. Correspondence, papers, records, and any other items showing employment or lack of employment.

18. Telephone books, and/or address books, facsimile machines to include the carbon roll and/or other memory system, any papers reflecting names, addresses, telephone numbers, pager numbers, cellular telephone numbers, facsimile, and/or telex numbers, telephone records and bills relating to co-conspirators, sources of supply, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists. Also, telephone answering devices that record telephone conversations and the tapes therein for messages left for or by co-conspirators for the delivery or purchase of controlled substances or laundering of drug proceeds.

19. Safes and locked storage containers, and the contents thereof which are otherwise described in this document.

20. Tools: Tools that may be used to open hidden compartments in vehicles, paint, bonding agents, magnets, or other items that may be used to open/close said compartments.

21. The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 21 U.S.C. § 841(a)(1), Distribution of Controlled Substances, 21 U.S.C. § 846, Conspiracy to Distribute Controlled Substances, 21 U.S.C. § 843(b), Use of a Communications Facility in Furtherance of a Felony Drug Offense, and 18 U.S.C. § 1956, Conspiracy to Launder Monetary Instruments:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. All records relating to violations of 21 U.S.C. § 841(a)(1), Distribution of Controlled Substances, 21 U.S.C. § 846, Conspiracy to Distribute Controlled Substances, 21 U.S.C. § 843(b), Use of a Communications Facility in Furtherance of a Felony Drug Offense, and involving Devin Vassallo since 2017, including:

i. lists of customers and related identifying information;

ii. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

iii. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

iv. any information recording Devin Vassallo's schedule or travel from 2017 to the present;

v. all bank records, checks, credit card bills, account information, and other financial records.

22. Digital devices[1] or other electronic storage media[2] and/or their components, which include:

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

23. Any digital devices or other electronic storage media that were or may have been used as a means to commit the offenses described on the warrant, including 21 U.S.C. § 841(a)(1), Distribution of Controlled Substances, 21 U.S.C. § 846, Conspiracy to Distribute Controlled Substances, 21 U.S.C. § 843(b), Use of a Communications Facility in Furtherance of a Felony Drug Offense.

24. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970